ABSTRACT:

The invention relates to a method of generating a random-number sequence, and to a random-number generator, particularly for a chip card or a smart card. The random-number generator comprises:

- a predetermined number Nosz of mutually independent frequency oscillators (10, 12),
- a predetermined number Nosz of flip-flops (14, 16), in which an output (26) of a frequency oscillator (10, 12) is connected to an input D (30) of a flip-flop (14, 16),
- a logic circuit element (18) receiving outputs Q (32) of the flip-flops (14, 16) as input values (36, 38) and, in accordance with a predetermined logic operation, assigns an output value (40) to these input values (36, 38),
- a parity circuit (20) determining the parity of a predetermined number Nlog of output values (40) from the logic circuit element (18),
- a random-number register (22) which buffers a predetermined number Nz of parity numbers (44) from the parity circuit (20) and supplies them as Nz bit random number, and an input (58) for an external clock signal source which clocks the flip-flops (14, 16), the parity circuit (20) and the random-number register (22).

Figure